# Frequently Asked Questions
# WPA2 Vulnerability (KRACK)

Release Date: **October 20, 2017**
Document version: **1.0**

## What is the issue?

A research paper disclosed serious vulnerabilities in the WPA and WPA2 key exchange mechanisms. Specifically, it was demonstrated that a sophisticated attacker with specialized tools within the range of a victim (wireless client) could potentially exploit any one of ten identified vulnerabilities to decrypt AES packets between a client and an AP.

Each of the ten vulnerabilities (see the list of CVE IDs in the KRACK link below) represents an individual avenue of potential attack that can be fixed by a software patch or mitigated. Most attacks, were they to occur, would be carried out by introducing a rogue AP to the network, tricking clients into connecting to the rogue AP, then performing a Key Reinstallation Attack (KRACK) as described in detail at the website https://www.krackattacks.com/.

Practically speaking, all ten identified vulnerabilities are subject to a hypothetical attack that is some variation of a compromise of 4-way and/or group key handshakes. In all ten cases, it is the client device that would be hypothetically hacked. In nine cases, only the client is the source of risk.

Only one of the ten attack vectors (CVEs) applies to an access point. The attack leverages a weakness in the 802.11r fast-transition protocol (a.k.a. fast roaming). Even in this case, the client device is the element subject to hypothetical attack.

*No attacks that exploit any identified vulnerabilities have been publicly reported.*

## Should I turn off WPA2?

No. The security risk posed by turning off WPA2 in favor of WPA1, WEP or Open is far greater than the risk associated with these newly identified vulnerabilities.

## What is potentially at risk? My network? The traffic on the network? Both?

Under no known circumstances is the network at risk.

The primary hypothetical risk is that an attacker could exploit the WPA2 implementation vulnerabilities exposed in this research to decrypt and replay packets sent from client to AP, i.e. user traffic could be intercepted. Packets cannot be forged or modified by the attacker and injected into the network. Not all vulnerabilities would allow for this.

None of the identified vulnerabilities provide a means of penetrating or undermining the network. None of the attacks allow a compromise of any passwords or certificates. None of the attacks can breach security of data transferred over end to end encrypted connections such as HTTPS, SSL, VPN, or IPSec.

## What would it take for an attacker to exploit any of these vulnerabilities?

The potential attacks outlined in the paper are very sophisticated and require specialized hardware and software. There is currently no publicly available code that enables this attack.

An attacker would need to develop and present a “fake” AP which impersonates the MAC address of a legitimate AP towards the client device (e.g. phone, laptop), but on a different channel from the legitimate AP, thus becoming a “man-in-the-middle” (MITM). Specialized software is needed to exploit the vulnerability that causes the same key/nonce combination to be used more than once. Additional tools are needed to extract the necessary information from the reused key/nonce combination in order to decrypt or replay subsequent client-AP communications.

## How at-risk am I with my Ruckus infrastructure?

The fact remains that no successful attacks have been reported and the difficulty of carrying out such an attack is extremely high. Hence, we assess the overall risk for any network as relatively low compared to any number of known risks, notably those associated with WPA1 and WEP.

Ruckus APs are not vulnerable to an attack that seeks to compromise 4-way and group key handshakes, as Ruckus APs store the latest value of the replay counter which will reject any messages that contain a different replay value.

Unpatched Ruckus APs (and all other unpatched vendor APs) are vulnerable to an attack based on 802.11r vulnerability. This is easily addressed, as described in, “how can I address the risk?” below.

Unpatched Ruckus APs making use of mesh networking functionality and unpatched Ruckus bridges (point-to-point / point-to-multipoint) are also vulnerable. Vulnerability in these deployments can be mitigated, as described in, “how can I address the risk?” below.

## How can I address the risk prior to infrastructure or client updates?

Recommendations for Ruckus infrastructure

**1. Eliminate the vulnerability associated with 802.11r by turning off 802.11r.** By default, this feature is disabled on both Ruckus controller-managed APs and Unleashed APs, and is disabled and not configurable on the Ruckus Cloud. For all client-to-AP scenarios, this fix is as good as a patch with the only downside being that 802.11r is disabled. There are two Ruckus-specific scenarios, described below, that are not addressed by this fix.

**2. Enable rogue detection mechanisms and ensure clients connecting to a rogue AP are de-authenticated.** This protects clients from malicious rogue APs. Ruckus products include this feature (labeled as "protect the network from malicious rogue access points" within the product).

**3. For cases in which mesh or bridging connections are used, configuring static channels and disabling background scanning will mitigate risk but will not eliminate it.** The nature of the Ruckus mesh implementation, in combination with rogue AP detection and remediation yields what Ruckus assesses to be an extremely low risk of exploit. Absolute remediation requires a software update.

Recommendation for client devices:

Apply security patches from device vendors such as Google, Microsoft, Apple, and Samsung as soon as they are available. At the time of this writing, patches are available for Windows 10 & 7 devices. The latest version of iOS is vulnerable only to 802.11r compromise. The researches that identified the vulnerabilities estimate that that 41% of Android devices are vulnerable and that a large proportion of IoT devices are vulnerable, as well.

A list of wireless vendors and the availability of software updates can be found on GitHub: https://github.com/kristate/krackinfo.

## What additional recommendations or tips can you offer?

- Do not use WEP, WPA1 or open networks as a replacement for WPA2. WPA2 is still the most secure choice.
- Since KRACK requires physical proximity by the attacker, double-check all physical security processes as and ensure that employees and other users are aware.

## How is this even possible – isn't WPA2 secure?

WPA2 uses the AES-CTR standard to encrypt data over an AP-client connection. To remain secure, AES-CTR requires that a combination of a specific key and nonce (an arbitrary number that may only be used once) value be used to encrypt a block of plaintext. If used more than once, an attacker could use these multiple instances to decrypt the plaintext. According to the research, vendor implementations of WPA2 can be exploited to use the same key and nonce value multiple times.

## There are multiple versions of WPA - Enterprise and PSK. Which are affected?

All versions of WPA and WPA2 are vulnerable, including WPA-Personal (PSK) and WPA2-Personal as well as WPA-Enterprise (802.1X) and WPA2-Enterprise.

## Do I need to change my passwords or pre-shared keys?

These vulnerabilities do not allow for the exposure of authentication credentials such as passwords and pre-shared keys. Thus, there is no need to change passwords and pre-shared keys due to the identified vulnerabilities, even on exposed networks.

## Why are mesh and point-to-point uniquely affected?

The open source Linux WPA supplicant utility is another instance of a WPA2 implementation that is susceptible to these vulnerabilities. Many APs (including Ruckus APs) use this utility in mesh and point-to-point connections, in which one AP acts as the supplicant.

## Which Ruckus products and releases are affected?

All unpatched Ruckus APs are vulnerable if 802.11r is enabled and/or if mesh is enabled. Ruckus bridge products are also affected.

802.11r is supported by all APs (but disabled by default) in the following releases:

- SmartZone 3.4 and newer
- ZoneDirector – all supported releases
- Unleashed
- Ruckus Cloud (disabled, not configurable)

Mesh is supported by all APs except for R300, R310, and H320.

## What is Ruckus doing to address these vulnerabilities?

Ruckus will be releasing software (patches) to address 802.11r, mesh, and point-to-point networking-related vulnerabilities. These vulnerabilities are the result of an implementation factor that allows multiple uses of the same key and nonce pair, thus exposing supplicants found in clients, mesh APs, and point-to-point links. In addition to addressing the network-side vulnerability, Ruckus intends to address the vulnerability of unpatched clients connected to Ruckus APs as an optional configuration. If this optional configuration is used, there may be a performance downside. Ultimately, both the infrastructure and clients will need to be patched in order to be fully protected from these vulnerabilities while providing full performance and network functionality.

Patches will be issued on the following software releases:

- SmartZone releases 3.1.2, 3.2.1, 3.4.2, and 3.5.1
- ZoneDirector releases 9.10.2, 9.12.3, 9.13.3, and 10.0.1
- Ruckus Cloud
- Unleashed 200.5
- P300 release 100.1
- 7731: Release TBD

Patch availability dates are provided in security bulletin ID 101617 located at https://www.ruckuswireless.com/security.

All subsequent releases will include the necessary fixes.

## Will upgrading my Ruckus network eliminate the vulnerability?

Ruckus software updates will address the infrastructure side of the Wi-Fi network and will provide a configurable option to address client vulnerabilities when connecting to the Ruckus network, however this will come with the tradeoff of potentially reducing performance. To avoid this tradeoff and protect the client when connecting to other networks, Ruckus recommends that customers review information shared by vendors of the Wi-Fi clients used on the network to assess impact and mitigation paths.

Check vendor patch status at https://github.com/kristate/krackinfo. The vendor's own web site and security advisory should always be considered the final authority regarding status.

## What if I don't have an active Support contract with Ruckus – will I be able to upgrade my software?

Yes, Ruckus will enable customers without active Support contracts to upgrade to a release that addresses these vulnerabilities.

## Does Ruckus have a security advisory detailing this?

Yes. Please find Ruckus security advisory on the support site and here:
https://www.ruckuswireless.com/security

## How can I find out more?

Ruckus blog on this topic: https://theruckusroom.ruckuswireless.com/wi-fi/2017/10/16/commonsense-approach-uncommon-problem/

Mathy Vanhoef's original research paper "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2": https://papers.mathyvanhoef.com/ccs2017.pdf